IN THE CLAIMS

Please amend the claims, as follows:

1. (Currently amended) A method comprising:

forwarding peer-to-peer content in a wireless network having a network infrastructure, where a wireless sender encrypts protected content or content encryption key and a wireless recipient consumes the protected content without requiring ~~content personalization~~ assistance from the network infrastructure~~; and~~

~~sending an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient~~.

2. (Canceled) A method according to claim 1, **characterized in that** the wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient.

3. (Currently amended) A method according to claim 1~~2~~, wherein the wireless recipient sends a device certificate having a public key to the wireless sender.

4. (Previously presented) A method according to claim 3, wherein the wireless sender personalizes the protected content or content encryption key for the wireless

recipient.

5. (Previously presented) A method according to claim 4, wherein the personalizing includes:

encrypting the content or content encryption key using the public key of the wireless recipient;

signing encrypted content or content encryption key using a private key of the wireless sender; and

sending the protected content or content encryption key together with a device certificate of the wireless sender to the wireless recipient.

6. (Previously presented) A method according to claim 4, wherein the wireless recipient verifies forwarded protected content received from the wireless sender by:

verifying the device certificate of the wireless sender; and

applying a private key of the wireless recipient in order for the recipient to consume the protected content.

7. (Previously presented) A method according to claim 1, wherein the protected content is digital rights management protected content.

8. (Currently amended) A wireless network comprising:

at least two wireless terminals;

a network infrastructure for forwarding peer-to-peer content from one wireless terminal to another wireless terminal;

the at least two wireless terminals having a peer-to-peer forwarding/reception of DRM protected content module configured for either encrypting or consuming protected content without ~~content personalization~~ assistance from the network infrastructure;

~~the peer-to-peer forwarding/reception of DRM protected content protocol module of a wireless sender configured for sending an initial message having either an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.~~

9. (Canceled) A wireless network according to claim 8, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content protocol module of a wireless sender sends an initial message having either an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

10. (Previously presented) A wireless network according to claim 8, wherein the peer-to-peer forwarding/reception of DRM protected content module of the wireless recipient is configured to send a device certificate having a public key to the wireless sender.

11. (Previously presented) A wireless network according to claim 8, wherein the peer-to-peer forwarding/reception of DRM protected content module of the wireless sender is configured to personalize the protected content or content encryption key for the wireless recipient.

12. (Previously presented) A wireless network according to claim 11, wherein the peer-to-peer forwarding/reception of DRM protected content module of the wireless sender is configured to personalize the content or content encryption key for the wireless recipient by:

encrypting the content or content encryption key using a public key of the wireless recipient;

signing encrypted content or content encryption key using a private key of the wireless sender; and

sending the protected content or content encryption key together with a device certificate of the wireless sender to the wireless recipient.

13. (Previously presented) A wireless network according to claim 8, wherein the peer-to-peer forwarding/recipient of DRM protected content module of the wireless recipient is configured to verify forwarded protected content from the wireless sender by:

verifying a device certificate of the wireless sender; and

applying a private key of the wireless recipient in order for the wireless recipient to consume the protected content.

14. (Previously presented) A wireless network according to claim 8, wherein the protected content is digital rights management protected content.

15. (Currently amended) A wireless terminal comprising:

one or more modules for operating in a wireless network having another wireless terminal and a network infrastructure for forwarding peer-to-peer content from the wireless terminal to the other wireless terminal,

each wireless terminal having a peer-to-peer forwarding/reception of DRM protected content module configured for either encrypting, consuming, or a combination thereof, protected content without ~~content personalization~~ assistance from the network infrastructure~~, and~~

~~the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender configured for sending an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient~~.

16. (Canceled) A wireless terminal according to claim 1, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

17. (Previously presented) A wireless terminal according to claim 15, wherein the peer-to-peer forwarding/reception of DRM protected content module of the wireless sender is configured to personalize the protected content for the wireless recipient.

18. (Previously presented) A wireless terminal according to claim 17, wherein the peer-to-peer forwarding/reception of DRM protected content module of the wireless sender is configured to personalize the content for the wireless recipient by:

encrypting the content or content encryption key using a public key of the wireless recipient;

signing encrypted content or content encryption key using a private key of the wireless sender; and

sending the protected content or content encryption key together with a device certificate of the wireless sender to the wireless recipient.

19. (Previously presented) A wireless terminal according to claim 15, wherein the peer-to-peer forwarding/reception of DRM protected content module of the wireless recipient is configured to send a device certificate having a public key to the wireless sender.

20. (Previously presented) A wireless terminal according to claim 15, wherein the peer-to-peer forwarding/recipient of DRM protected content module of the wireless recipient is configured to verify forwarded protected content from the wireless sender by:

verifying a device certificate of the wireless sender; and

applying a private key of the wireless recipient in order for the wireless recipient to consume the protected content.

21. (Previously presented) A wireless terminal according to claim 15, wherein the protected content is digital rights management protected content.

22. (Currently amended) A method comprising:

forwarding a protected content or content encryption key from a first terminal to a second terminal;

~~sending an initial message from the first terminal to the second terminal, the initial message including a sender name, an international mobile equipment identity, a mobile station integrated service digital network number, or a combination thereof;~~

sending a digital rights management device certificate containing a public digital rights management key from the second terminal to the first terminal;

verifying the public digital rights management key by the first terminal;

personalizing digital rights management content or content encryption key by encryption using a public key of the second terminal;

signing encrypted digital rights management content or content encryption key using a private digital rights management key of the first terminal;

sending encrypted and signed digital rights management content or content encryption key together with a digital rights management device certificate of the first terminal from the first terminal to the second terminal;

verifying the digital rights management device certificate of the first terminal by the second terminal; and

applying a private digital rights management key of the second terminal, if the private digital rights management key of the first terminal is verified, in order for the second terminal to consume the protected content.

23. (Canceled) A method according to claim 22, **characterized in that** the initial message includes a sender name, an international mobile equipment identity, a mobile station integrated service digital network number, or a combination thereof.

24. (Currently amended) A method according to claim 22~~23~~, wherein the method further comprises confirming receipt of the encrypted and signed digital rights management content or content encryption key from the second terminal to the first terminal.

25. (Previously presented) A method according to claim 24, wherein the method further comprises sending an error message if verification of the encrypted and signed digital rights management content or content encryption key fails.

26. (Previously presented) A method according to claim 22, wherein the sender sends the initial message having a device certificate to the second terminal.

27. (Previously presented) A method according to claim 1, wherein the initial message includes a device certificate to the wireless recipient.

28. (Currently amended) Apparatus comprising:

means for forwarding peer-to-peer content in a wireless network having a network infrastructure; and ~~by~~

means for encrypting protected content or content encryption key in a wireless sender so a wireless recipient can consume the protected content without requiring ~~content personalization~~ assistance from the network infrastructure~~; and~~

~~means for sending an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient~~.

29. (New) Apparatus according to claim 28, wherein the apparatus further comprises:

means for sending an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient

30. (New) A method according to claim 1, **characterized in that** the wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient.

31. (New) A wireless network according to claim 8, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content protocol module of a wireless sender sends an initial message having either an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

32. (New) A wireless terminal according to claim 15, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

33. (New) A method according to claim 22, **characterized in that** the initial message includes a sender name, an international mobile equipment identity, a mobile station integrated service digital network number, or a combination thereof.

34. (New) A method according to claim 1, wherein the wireless sender personalizes the protected content or content encryption key for the wireless recipient.